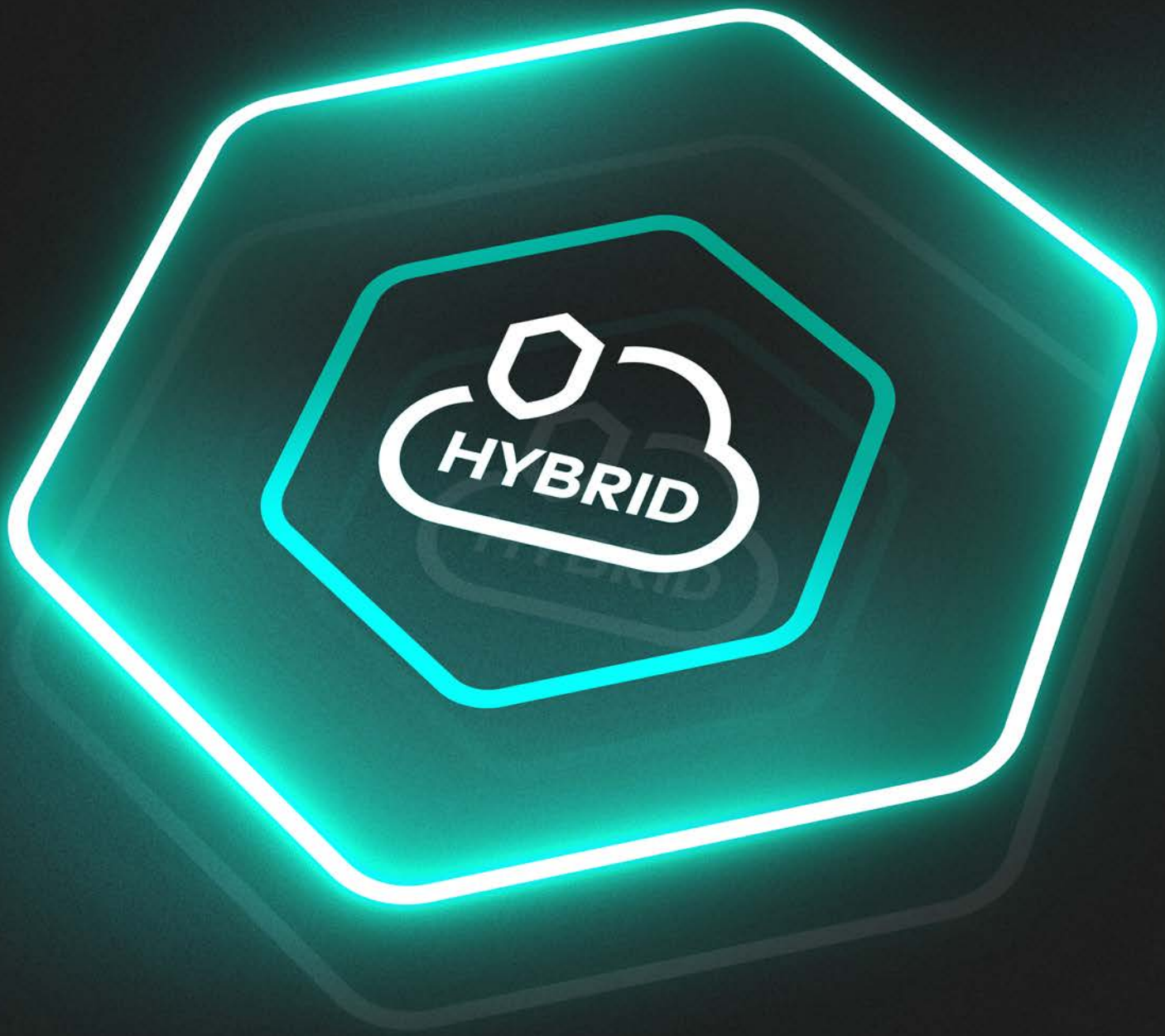


Kaspersky Hybrid Cloud Security

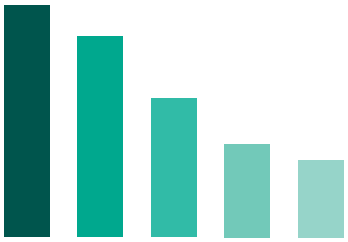
kaspersky BRING ON THE FUTURE

今日の企業はデジタル変革に注視しており、それが急速なクラウド導入の要因となっています。これらの取り組みは効率の向上など、企業に多くの利点をもたらす一方で、インフラストラクチャをますます複雑なものにして、セキュリティリスク、ガバナンス、スタッフリソース、パフォーマンスの最適化、新しい法規制、および費用の面で大きな問題を生じさせます。Kaspersky Hybrid Cloud Security はこれらすべての課題に対処します。

実績のあるクラウドネイティブ保護とハイブリッド環境に最適なパフォーマンス

Kaspersky Hybrid Cloud Security により、クラウド導入、デジタル変革、およびビジネス全般がより安全かつ効率的になります。単一の製品でハイブリッドインラフストラクチャ全体を保護して、リスクを軽減し、仮想リソースの消費を低減し、法規制のコンプライアンスをサポートすることができます。Kaspersky Hybrid Cloud Security は、可視化を高めて管理を簡素化しながら、お客様とお客様の大切な時間と予算リソースを守ります。セキュリティの懸念が解消されるため、デジタル変革プロセスの他の側面に集中できるようになります。

クラウドに関する主な課題



- セキュリティ　**81%**
- クラウド費用の管理　**79%**
- ガバナンスとコンプライアンス　**75%**
- マルチクラウドの管理　**72%**
- クラウド移行　**71%**

出典：Flexera State of the Cloud Report（2021 年）

ハイブリッド環境のセキュリティリスクに対処する最高レベルの保護性能

- 多層型の脅威保護が、マルウェア、フィッシングなどを含む広範囲のサイバー攻撃を早期に阻止します。
- 人間の専門知識と機械学習を組み合わせることで、誤検知を最小限に抑えて最高レベルの検知を実現します。
- リアルタイムの脅威インテリジェンスデータが最新のエクスプロイトからの防御に役立ちます。

ハイブリッドインフラストラクチャのセキュリティパフォーマンスを最大限に高めるクラウドネイティブアプローチ

- サイバーセキュリティエンジンが、ワークロードを問わず（物理または仮想ワークロード、あるいはプライベートクラウド、パブリッククラウド、ハイブリッドクラウド上のワークロードなど）、ハイブリッドインフラストラクチャ全体を保護します。
- プラットフォームに依存しないアプローチをネイティブ統合と組み合わせることで、パブリッククラウドが DevOps に完全に対応します。
- OS に応じて最適化された Light Agent が仮想化リソースの消費を効率的に最大 30% 削減し、他の業務で利用できるように解放します。

コスト効率と利便性の高い管理により、快適なクラウド導入を実現

- 柔軟なライセンスモデルにより、必要な機能だけを選択して、セキュリティ予算を最大限に活用できます。
- 統合されたクラウドコンソールによって、インフラストラクチャ全体のセキュリティ管理を簡素化し、価値ある IT スタッフリソースを削減します。
- シンプルなクラウドインフラストラクチャインベントリと、エージェントの場所を問わない自動化されたセキュリティプロビジョニングの両方が、可視性を最大限に高めます。

規制の厳しい業界のコンプライアンスに対応するセキュリティ

- 適応性の高い多角的な製品が、システム堅牢化、エージェントによるセルフディフェンス、脆弱性評価、自動パッチ管理などのテクノロジーを利用して、お客様が法規制を完全に遵守できるよう継続的にサポートします。
- 幅広い機能により、コンプライアンスとリスク状況への適応を可能にして、常に最新の法規制に則ったセキュリティ態勢を確保します。

主な機能

多層型脅威対策

グローバルな脅威インテリジェンス	脅威の状況が変化している状況でも、リアルタイムにデータを収集します。
機械学習	機械学習のアルゴリズムと人間の専門知識を組み合わせることで、グローバルな脅威インテリジェンスのビッグデータを後押しします。
Web 上の脅威やメールによる脅威からの保護	仮想デスクトップやリモートデスクトップをメールや Web からもたらされる脅威から守ります。
Windows イベントログ監視	サイバー攻撃の可能性がある異常な動作がないか、内部ログファイルをスキャンします。
ふるまい分析	アプリケーションやプロセスの監視によって、ボディレスのマルウェアやスクリプトベースのマルウェアなど高度な脅威から守ります。
修復エンジン	必要に応じて、クラウドワークロード内で行われた悪意のある変更をロールバックします。
脆弱性攻撃ブロック	保護されたアプリケーションと完全に互換性のある状態で、脅威の侵入から効果的に守る保護を提供し、パフォーマンスに及ぼす影響を最小限に抑えます。
アンチランサムウェア機能	遠隔で開始された暗号化のブロックや影響を受けたファイルの暗号化前の状態へのロールバックなどを行い、身代金を要求するあらゆる試みから業務上重要なデータを守ります。
ネットワーク脅威対策	ネットワークからクラウド資産への侵入を検知して阻止します。
コンテナ保護	攻撃を受けたコンテナを介して感染がハイブリッド IT インフラストラクチャに移るのを防ぎます。

システム堅牢化により復元力を強化

アプリケーションコントロール	最適なシステム堅牢化を行うためにすべてのハイブリッドクラウドワークロードをデフォルト拒否モードでロックダウンして、動作するアプリケーションの範囲を正当で信頼できるものだけに限定できます。
デバイスコントロール	クラウドワークロードにアクセスできる仮想デバイスを指定します。
Web コントロール	仮想デスクトップとリモートデスクトップによる Web リソースの使用を制限することで、リスクを低減し、生産力を向上させます。
ホストベース侵入防止システム (HIPS)	起動されるアプリケーションに対して信頼カテゴリをあてはめ、重要リソースへのアクセスを制限して機能を限定することができます。
ファイル変更監視	重要システムのコンポーネントやその他の重要ファイルの整合性を確保するのに役立ちます。
脆弱性診断とパッチ管理	脆弱性診断、パッチとアップデートの配信、インベントリ管理、アプリケーションの展開など、セキュリティ、システム設定、管理に関する必要不可欠な作業を一元化し、自動化します。

ボーダレスな可視性

セキュリティの一元管理	オフィス、データセンター、クラウドなど、インフラストラクチャ全体のエンドポイントとサーバーを、単一のコンソールを使って管理できます。
クラウド API	パブリック環境とのシームレスな統合により、インフラストラクチャの検知、自動化されたセキュリティエージェントの展開、ポリシーベースの管理が可能になるほか、インベントリやセキュリティのプロビジョニングが容易になります。
柔軟な管理オプション	マルチテナンシー機能、権限ベースのアカウント管理、役割ベースのアクセス制御を備え、単一サーバーからの統合オーケストレーションの利点を維持して、柔軟性を実現します。
SIEM 統合	セキュリティ情報および管理システムとの製品統合を可能にし、ハイブリッド IT ネットワークにわたる企業のサイバーセキュリティの異なる側面を 1 か所にまとめます。

Kaspersky Hybrid Cloud Security が選ばれる理由

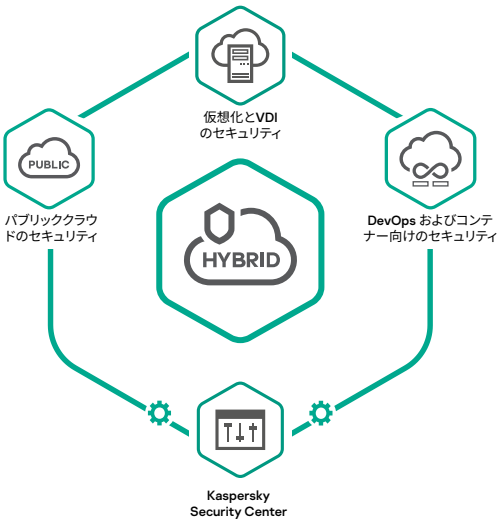
30%

節約できる可能性のある仮想ハードウェアリソース（従来のエンドポイントセキュリティソリューションを使用する場合と比較）

トップ 3

優れたパフォーマンスを維持。例年に続き昨年も、カスペルスキー製品は複数の独立テストに参加し、1 位に 57 回輝き、トップ 3 に 63 回入るという並外れたパフォーマンスを示しました（詳細は kaspersky.co.jp/top3 をご覧ください）。

単一の製品で組織の IT セキュリティのあらゆるニーズに対応



1 つの製品 | 1つのコンソール | 1つのライセンス

カスタマーレビュー

「このソリューションは、システムパフォーマンスに影響を及ぼしたり、ユーザーエクスペリエンスを損ねたりすることなく、仮想環境およびクラウド環境を保護します」

「1 つのライセンスですべてのセキュリティソリューションを組み合わせる素晴しい方法です」

「その他のアンチウイルスソフトウェアやその他のエージェントをインストールする必要はありません」

「データ保護のための一元化されたクラウドソリューションがすべて 1 か所にまとまっています」

「新しい更新をダウンロードする必要がまったくないので、保護機能は即座にすべての仮想マシンに適用されます」

「管理者が長期間のトレーニングを受けることなく使える最適なソリューション」

Amazon および Gartner のレビューから引用

デモのご依頼はこちら

www.kaspersky.co.jp